538,556

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 July 2004 (01.07.2004)

PCT

(10) International Publication Number
WO 2004/056036 A1

(51) International Patent Classification⁷: H04L 9/06

(21) International Application Number: PCT/IB2003/005508

(22) International Filing Date: 28 November 2003 (28.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/433,365 13 December 2002 (13.12.2002) US
60/473,527 27 May 2003 (27.05.2003) US

(71) Applicant (*for all designated States except US*): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): SEXTON, Bonnie, C. [US/US]; P.O. Box 32001, Briarcliff Manor, NY 10510-8001 (US).

(74) Common Representative: KONINKLIJKE PHILIPS ELECRONICS N.V.; c/o Waxler, Aaron, P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (NL).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

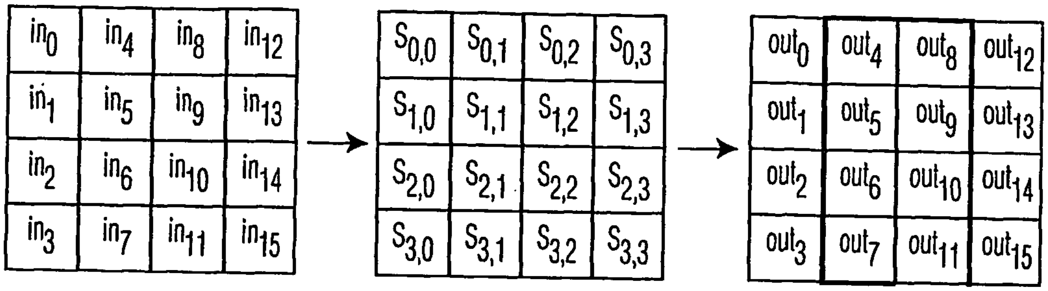
(84) Designated States (*regional*): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A SMALL HARDWARE IMPLEMENTATION OF THE SUBBYTE FUNCTION OF RIJNDAEL



(57) Abstract: A small hardware implementation is provided for the Advanced Encryption Standard SubByte function that implements the affine transform and inverse transform in a single Affine-All transform using a multiplicative inverse ROM. The logic is greatly reduced and the maximum path delay is reduced compared to a multiplexor implementation and is slightly greater than a ROM implementation.

WO 2004/056036 A1